UNIVERSITY of DENVER	**UNIVERSITY OF DENVER POLICY MANUAL INFORMATION SECURITY**

Responsible Department: Information Technology **Recommended By:** Provost, VC Business and Financial Affairs **Approved By:** Chancellor	**Policy Number** 1.10.080	**Effective Date** 6/8/2018

I. INTRODUCTION

The University information systems collect, manage, and store sensitive information on a regular basis in order to support business operations. The University is committed to preserving the confidentiality, integrity, and availability of its information resources while also preserving and nurturing the open, information-sharing requirements of its academic culture. The University must protect its information assets, provide for the integrity of institutional processes and records, and comply with applicable laws and regulations.

II. POLICY OVERVIEW

The purpose of this Policy is to:

1. Ensure the University's compliance with applicable laws and regulations, and support the implementation of information security best practices.

2. Authorize the creation of the University Information Security Program, (the "Program") in support of this Policy. The Program will establish, implement, and maintain information security related policies, procedures and standards for the University. These documents will be consolidated in the University's "Information Security Policy Manual" for ease of use and simplified maintenance.

3. Authorize the creation of the University Information Security Steering Committee, (the "ISSC") in support of this policy and the Program. The ISSC will develop, review, and maintain information security policies and standards. The ISCC will provide guidance and support to the University's Associate Vice Chancellor for Information Technology ("AVC for IT") and Chief Information Security Officer ("CISO") for the maintenance of the Program on behalf of the Executive Risk and Compliance Committee ("ERCC").

III. PROCESS OVERVIEW

A. Policy Statement

The University is committed to protecting information assets in accordance with applicable legal, regulatory, contractual and grant compliance requirements. The University is dedicated to collecting, handling, storing and disposing of sensitive information properly and securely. The Information Security Policy creates an Information Security Program that ensures the following:

1. **Compliance** - The University will develop, implement, and manage the processes and procedures necessary to ensure that it complies with all applicable legal, regulatory, grant and contractual obligations relating to information security. *(Information Security Policy Manual section 15.0).*

2. **Risk assessments** – The University will perform periodic risk assessments, as defined in the Information Security Policy Manual, to identify and remediate risks that may threaten the confidentiality, integrity, or availability of University information systems and sensitive data. Risk assessments will evaluate the existing policies, procedures, technology solutions, and other arrangements to determine the effectiveness of the controls and will make recommendations for changes and improvements. *(Information Security Policy Manual section 4.0).*

3. **Policy development and maintenance** - The University will maintain appropriate subordinate policies, procedures, standards, and other materials sufficient to create, implement, and maintain the Program. These supporting elements will be developed by the ISSC and approved by the ERCC prior to implementation. These supporting elements will be periodically updated to reflect changes in technology and the University. *(Information Security Policy Manual section 5.0).*

4. **Vulnerability assessment and management** - The University will establish, implement, and maintain a risk-based testing program to periodically evaluate controls, systems, and procedures of the Program and confirm the controls are effective. Such controls, systems, and procedures will be subject to periodic testing by outside auditors selected in conjunction with the Internal Audit Department and approved the by the Audit Committee. *(Information Security Policy Manual section 12.6)*

5. **Incident prevention and response handling** - The University will establish, implement, and maintain prevention and response programs to appropriately react and respond to potential and real-time threats to University information assets. This will include formation of an Incident Response Team ("IRT") function as detailed in the Information Security Policy Manual. *(Information Security Policy Manual section 13.0).*

6. **Monitoring and reporting** - The University will constantly monitor and periodically report on elements of the Program and overall security posture of the University. This information will be provided to the Audit Committee of the Board of Trustees, senior staff, or other groups as requested. *(Information Security Policy Manual section 10.10).*

7. **Organization of information security** – The University will develop and implement a reporting structure that will define responsibilities for defining technical and non- technical information security standards, procedures and guidelines on an enterprise wide basis. These responsibilities will be distributed among members of the ISSC and reviewed/updated regularly as detailed in the Information Security Policy Manual. *(Information Security Policy Manual section 6.0).*

8. **Asset management** - The University will identify and actively manage its Significant Information Assets. Significant Information Assets are those assets having an aggregate replacement value of at least $50,000, whether individually or in related groups, and includes computer hardware and software providing a specific IT service. The AVC for IT and the CISO, or designee, will maintain an accurate and complete inventory of all Significant Information Assets. The inventory will include information about Significant Information Asset owners, security classifications, asset locations, asset values, operating systems, versions, and other relevant information. Among other things, capturing and analyzing this information will allow for an understanding of asset values in order to maintain appropriate protection. *(Information Security Policy Manual section 7.0).*

9. **Human Resources security** - The University will develop and maintain policies and procedures to ensure that all persons accessing University information systems comply with University information security principles, policies, standards, procedures and guidelines, plus requirements identified in the terms and conditions of their employment or service contracts, and applicable laws and regulations. The University will ensure that all persons accessing University information systems receive appropriate training and regular updates in information security policies, standards, procedures, laws, and regulations where relevant to their job functions and systems access. Where applicable, this training includes security requirements, legal responsibilities and business controls (such as security incident reporting processes), as well as induction training in the appropriate and secure use of IT facilities before access to information or IT services is granted. *(Information Security Policy Manual section 8.0).*

10. **Physical and environmental security** - The University will develop and implement processes and procedures necessary to ensure information assets are housed securely and protected against identified risks. *(Information Security Policy Manual section 9.0).*

11. **Communications and operations management** – The University will develop, implement, and manage the processes and procedures necessary to ensure changes to information processing facilities, equipment, systems, and applications are controlled through formal management responsibilities and procedures appropriate for the risks involved. *(Information Security Policy Manual section 10.0)*.

12. **Access control** – The University will develop, implement and maintain the processes and procedures necessary to ensure that access to information assets is only granted to authorized persons based on business and security requirements and the principals of "least privilege" and "minimum necessary". *(Information Security Policy Manual section 11.0)*.

13. **Information systems acquisition, development and maintenance** – The University will develop, implement, and manage the processes and procedures necessary to ensure that information security is taken into account early in the systems development lifecycle including business cases, budget proposals, and work requests, to minimize the overall security costs and ensure that sufficient resources are allocated to complete the necessary information security tasks. This applies to custom software developed in-house or externally and commercial off the shelf packages, both new systems and changes to existing systems. *(Information Security Policy Manual section 12.0).*

14. **Business continuity management** – The University will develop, implement, and manage the processes and procedures necessary to ensure that information systems are sufficiently resilient. This includes ensuring the continuity of critical University business processes despite minor incidents and ensuring proven disaster recovery arrangements are in place to minimize the impact of serious incidents. *(Information Security Policy Manual section 14.0)*.

The ISCC shall be responsible for implementation of policies and procedures, and management of processes related to Human Resources security, physical and environmental security, and communications and operations security. The AV for IT and the CISO shall lead the University's creation of processes and procedures necessary to implement other policy statements set forth in the preceding paragraphs.

B. ERCC Scope, Authority, and Responsibility

The ERCC is responsible for interpretation of, enforcement of, and approving revisions to exceptions to this policy, subordinate policies, and associated standards. The AVC for IT, or designee, is charged with leading and advising the ISSC in the development, implementation, and execution of the Program.

C. Information Security Program Principles

The Program is designed to address enterprise wide security compliance while retaining the flexibility required to address relevant changes in technology. The following guiding principles serve as the cornerstone upon which the Program is built: *(Information Security Policy Manual section 3.2.1)*

1. Information is a critical business asset of the University and must be protected to a degree appropriate to its vulnerability and its importance or value to the organization. This includes our information assets and those placed in our care.

2. Information security controls are necessary to protect our information assets against unacceptable risks to their confidentiality, integrity, and availability.

3. We invest wisely in proven information security controls where justified on the basis of lifecycle cost-benefit assessment and risk analysis.

4. Information security is pervasive throughout the entire organization. It is an inherent part of our information technology ("IT") architecture and a component of our operational and management processes. In short, we are *all* responsible for information security.

5. Information security is a core element of enterprise governance. It is closely related to aspects such as IT management, physical site security, risk management, legal and regulatory compliance and business continuity. It supports various obligations to our students, employees, business partners and to the community at large.

6. Information security is a business enabler that allows us to enter more confidently into and to maintain business relationships. Minimizing information security incidents supports our financial bottom line. It also enhances our image as a trustworthy, open, honest and ethical organization.

7. University information security policies and procedures conform to accepted best practice as defined by information security standards published by the International Organization for Standardization and the International Electro-Technical Commission, and other relevant information security standards.

8. The ISSC may consist of members from the following departments or areas, which may be modified as appropriate:

    i. Human Resources and Inclusive Community;

    ii. Office of General Counsel;

    iii. The Controller's Office;

    iv. The Provost's Office;

    v. The Office for Business & Finance Affairs;

    vi. Enterprise Risk Management;

    vii. Internal Audit;

    viii. Institutional Research and Analysis;

    ix. Office of the Registrar;

    x. Information Technology;

    xi. Campus Life and Inclusive Excellence; or

    xii. A faculty member.

For additional information, please use the Information Security Hotline: 303-871-4940

IV. DEFINITIONS

None